



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/675,262	09/28/2000	Jesse R. Walker	42390P9007	3019

8791 7590 04/21/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN  
12400 WILSHIRE BOULEVARD  
SEVENTH FLOOR  
LOS ANGELES, CA 90025-1030

EXAMINER

CHO, UN C

ART UNIT	PAPER NUMBER
----------	--------------

2687

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/675,262

Applicant(s)

WALKER, JESSE R.

Examiner

Un C Cho

Art Unit

2687

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 21 June 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 09 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Claim Objections***

1. Claim 22 is objected to because of the following informalities:

Regarding claim 22, line 2 of the claim recites "... the wirelessly station ...", it should be "... wireless station ..." instead.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 22, 23 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila et al. (US 6,587,680 B1) in view of Brown et al. (US 6,678,733 B1).

Regarding claim 1, Ala-Laurila discloses a method for establishing secured roaming among a wireless station, a first (old-AP, Fig. 2, 14) and a second access points (new-AP, Fig. 2, 114) comprising: the first access point requesting a first ticket from an authentication server and using the first ticket to establish a first secured session with the wireless station (there already exists a security association between the mobile terminal and the current or old-AP, Ala-Laurila, Col. 8, lines 1 – 6, every time a mobile station powers on it registers with

the base station in order to receive service, thus it is assumed that the first secured session has already been established with the mobile terminal prior to a second ticket request); and in response to a second ticket request from the wireless station through the first secured session, the first access point forwarding the second ticket request to the authentication server and relaying a resulting second ticket from the authentication server to the wireless station (mobile terminal indicating to the current or old-AP that handover is required and when the message is received by the old-AP it retrieves security association parameters, SA, from its security association database and relaying a response message to the mobile terminal, Ala-Laurila, Col. 10, lines 39 – 57).

However, Ala-Laurila does not specifically disclose that the second ticket being different than the first ticket, wherein the second ticket is used to establish a second secured session between the wireless station and the second access point. In an analogous art, Brown discloses that the second ticket (request access with ticket, Fig. 6, 610) being different than the first ticket (request access, Fig. 6, 616), wherein the second ticket is used to establish a second secured session between the user and the server (request access, first ticket, is just a request to gain access to a network but since there is no authentication the network denies access to the user, when the user request access with ticket, second ticket, the network grants access because it is already authenticated by the network, Brown, Col. 11, line 22 through Col. 13, line 25). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was

made to provide the technique of Brown to the system of Ala-Laurila in order to provide a method and system that authenticates users and authorizes the users to access the network for security purposes.

Regarding claim 22, Ala-Laurila in view of Brown as applied to claim 1 above discloses that the second ticket is only valid for the second secured session between the wireless station and the second access point (request access with ticket, having an expiration period, thus being only valid for the session between the user and the server, Brown, Col. 12, lines 3 – 13).

Regarding claim 23, Ala-Laurila in view of Brown as applied to claim 22 above discloses that the second ticket is only valid for the second secured session for a predetermined period of time (request access with ticket, having an expiration period, thus being only valid for the session between the user and the server, Brown, Col. 12, lines 3 – 13).

Regarding claim 27, the claim is interpreted and rejected for the same reason as set forth in claim 1.

4. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila in view of Brown as applied to claim 1 above, and further in view of Jetzek et al. (US 6,539,227 B1).

Regarding claim 2, Ala-Laurila in view of Brown as applied to claim 1 above does not specifically disclose applying the second ticket and a group identity shared by the first and the second access points to establish a second

secured session between the wireless station and the second access point, the group identity identifying that the first and second access points belong to the same group, and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket. In an analogous art, Jetzek discloses applying the second ticket (mobile station roaming from one base station to another performing handoff) and a group identity shared by the first and the second access points to establish a second secured session between the wireless station and the second access point, the group identity identifying that the first and second access points belong to the same group (groups of cells, base stations or other transmission sources having softzone identification number, softzone ID, Jetzek, Col. 6, line 66 through Col. 7, line 3), and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket (soft handoffs are permitted only between members within the group having the same softzone ID, Jetzek, Col. 7, lines 4 – 44). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the technique of Jetzek to the modified system of Ala-Laurila and Brown in order to provide methods and system to determine which handoff type is preferred at a specific location under current radio conditions and to control hard and soft handoff while at the same time minimizing the overhead signaling between the network and the mobile station.

Art Unit: 2687

5. Claims 3, 5 – 9, 11 – 13 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila et al. (US 6,587,680 B1) in view of Brown et al. (US 6,678,733 B1) as applied to claim 1 above and further in view of Brown et al. (US 5,689,563).

Regarding claim 3, Ala-Laurila in view of Brown as applied to claim 1 above does not specifically disclose that the authentication server dynamically generating a first and a second session keys to include in the first and the second tickets and the authentication server encrypting the first and the second tickets with a first and a second encryption keys. In analogous art, Brown (US 5,689,563) discloses that the authenticating unit generates a first and a second session keys to include in the first and the second tickets and the authenticating unit encrypting the first and the second tickets with a first and a second encryption keys (Brown, Col. 3, line 63 through Col. 4, line 8). Therefore, it would have been obvious to one of ordinary skill in the art the time the invention was made to provide the technique of Brown to the modified system of Ala-Laurila and Brown to create an encryption technique to alleviate problems associated with packetized data to be more efficient and secure.

Regarding claim 5, Ala-Laurila in view of Brown and further in view of Brown as applied to claim 3 above discloses the first fixed network communication unit 130 appending application specific information to the second ticket to formulate a combined message and the first fixed network

communication unit encrypting the combined message with the first session key (Brown (US 5,689,563), Col. 6, lines 35 – 54).

Regarding claim 6, Ala-Laurila in view of Brown and further in view of Brown (US 5,689,563) as applied to claim 5 above discloses the application specific information further comprises the first fixed network communication unit 130 selected instant specific information and random challenge (RAND) (Brown, Col. 6, lines 14 – 21 and Col. 7, lines 39 – 48).

Regarding claim 7, Ala-Laurila in view of Brown (US 6,678,733 B1) and further in view of Brown (US 5,689,563) as applied above discloses an access point (Fixed network communication unit, Brown (US 5,689,563), Fig. 1, 130) in a secured wireless roaming system, comprising an antenna (an antenna, Brown (US 5,689,563), Fig. 1, 154); a filter coupled to the antenna (inherently a filter coupled to the antenna), a receiver and a transmitter coupled to the filter (a receiver and a transmitter, Brown (US 5,689,563), Fig. 1, 152, coupled to the filter) and a control unit coupled to the receiver and the transmitter and coupled to a wired-network connection interface (microprocessor, Brown (US 5,689,563), Fig. 1, 148, coupled to the receiver and the transmitter, which forms a switch center, Brown (US 5,689,563), Fig. 1, 128, and the switch center is coupled to a wired-network such as PSTN, Brown (US 5,689,563), Fig. 1, 132), wherein the control unit further comprises an authentication protocol engine (switch center comprises a database, Brown (US 5,689,563), Fig. 1, 136, Brown (US 5,689,563), Col. 5, lines 54 – 66), that requests a first ticket from an

authentication server and uses the first ticket to establish a first secured session with a wireless station (subscriber unit and fixed network communication unit performs authentication to establish a secured session, Brown (US 5,689,563), Col. 6, lines 14 – 67); and in response to a second ticket request from the wireless station through the first secured session, forwards the second ticket request to the authentication server and relays a resulting second ticket from the authentication server to the wireless station (mobile terminal indicating to the current or old-AP that handover is required and when the message is received by the old-AP it retrieves security association parameters, SA, from its security association database and relaying a response message to the mobile terminal, Ala-Laurila, Col. 10, lines 39 – 57), the second ticket being different than the first ticket, wherein the second ticket is used to establish a second secured session between the wireless station and the second access point (request access, first ticket, is just a request to gain access to a network but since there is no authentication the network denies access to the user, when the user request access with ticket, second ticket, the network grants access because it is already authenticated by the network, Brown (US 6,678,733 B1), Col. 11, line 22 through Col. 13, line 25).

Regarding claim 8, Ala-Laurila in view of Brown and further in view of Brown (US 5,689,563) as applied to claim 7 above discloses that a switch center (Fig. 1, 128) decrypting the second ticket request (Brown (US 5,689,563), Col. 8, lines 16 – 24).

Regarding claim 9, the claim is interpreted and rejected for the same reason as set forth in claim 3.

Regarding claim 11, Ala-Laurila in view of Brown and further in view of Brown as applied to claim 8 above discloses that the first fixed network communication unit (Brown (US 5,689,563), Fig. 1, 130) appends application specific information to the second ticket to formulate a combined message with the first session key (Brown (US 5,689,563), Col. 6, lines 35 – 64).

Regarding claim 12, the claim is interpreted and rejected for the same reason as set forth in claim 6.

Regarding claim 13, Ala-Laurila in view of Brown (US 6,678,733 B1) and further in view of Brown (US 5,689,563) as applied above discloses a wireless station (subscriber unit, Brown (US 5,689,563), Fig. 1, 100) in a secured wireless roaming system comprising an antenna (an antenna, Brown (US 5,689,563), Fig. 1, 124); a filter coupled to the antenna (inherently a filter coupled to the antenna); receiver and a transmitter coupled to the filter (a receiver and a transmitter, Brown (US 5,689,563), Fig. 1, 122, coupled to the filter) and a control unit coupled to the receiver and the transmitter (a microprocessing stage, Brown (US 5,689,563), Fig. 1, 118, coupled to the receiver and the transmitter), wherein the control unit further comprises an authentication protocol engine (microprocessing stage coupled to the memory, Brown (US 5,689,563), Fig. 1, 106) that requests a second ticket from an authentication server via a first secured session established with a first access point using a first ticket (mobile terminal indicating

to the current or old-AP that handover is required and when the message is received by the old-AP it retrieves security association parameters, SA, from its security association database and relaying a response message to the mobile terminal, Ala-Laurila, Col. 10, lines 39 – 57), the second ticket being different than the first ticket and establishes a second secure session with a second access point using the second ticket received via the first secured session (request access, first ticket, is just a request to gain access to a network but since there is no authentication the network denies access to the user, when the user request access with ticket, second ticket, the network grants access because it is already authenticated by the network via the first secured session, Fig. 6, 616, 624, Brown (US 6,678,733 B1), Col. 11, line 22 through Col. 13, line 25).

Regarding claim 24, Ala-Laurila in view of Brown and further in view of Brown as applied to claim 3 above discloses that the first access point requesting a first ticket from an authentication server comprises the wireless station providing an identification of the wireless station to the first access point (every time the mobile station registers with a base station it inherently provides its identification number to the base station, Brown (US 5,689,563), Col. 7, lines 4 – 14); the first access point obtaining the first ticket from the authentication server (access point retrieves SA parameters from the security association data base, Fig. 5A, Ala-Laurila, Col. 10, lines 33 – 57); and the first access point establishing the first secured session using the newly obtained first ticket (access point

Art Unit: 2687

establishing secured session with mobile terminal, Ala-Laurila, Col. 8, lines 1 – 6).

6. Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila in view of Brown and further in view of Brown (US 5,689,563) as applied to claim 24 above, and further in view of Jetzek (US 6,539,227 B1).

Regarding claim 25, Ala-Laurila in view of Brown and further in view of Brown (US 5,689,563) as applied to claim 24 above does not specifically disclose the wireless station obtaining a group ID from the first access point via the first secured session, the group ID being shared with the first and second access points and identifying that the first and second access point belong to the same group, wherein the wireless station can only access another access point within the same group. In an analogous art, Jetzek discloses the wireless station obtaining a group ID from the first access point via the first secured session (obtaining the softzone IDs distributed from the network to the mobile station), the group ID being shared with the first and second access points and identifying that the first and second access points and identifying that the first and second access point belong to the same group (groups of cells, base stations or other transmission sources having softzone identification number, softzone ID, Jetzek, Col. 6, line 66 through Col. 7, line 3), wherein the wireless station can only access another access point within the same group (soft handoffs are permitted only between members within the group having the same softzone ID, Jetzek,

Col. 7, lines 4 – 44). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the technique of Jetzek to the modified system of Ala-Laurila, Brown and Brown in order to provide methods and system to determine which handoff type is preferred at a specific location under current radio conditions and to control hard and soft handoff while at the same time minimizing the overhead signaling between the network and the mobile station.

Regarding claim 26, Ala-Laurila in view of Brown, further in view of Brown (US 5,689,563) and further in view of Jetzek as applied to claim 25 above discloses that the second secured session is established based on the second session key (using session key, Brown (US 5,689,563), Col. 3, line 63 through Col. 4, line 8) and the group ID (using softzone identification number, Jetzek, Col. 7, lines 1 – 44).

7. Claims 4 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila in view of Brown and further in view of Brown (US 5,689,563) as applied to claim 3 above, and further in view of Hauser et al. (US 5,778,065).

Regarding claim 4, Ala-Laurila in view of Brown and further in view of Brown (US 5,689,563) as applied to claim 3 above does not specifically disclose that the first and second session keys have limited lifetime. In an analogous art, Hauser discloses that session keys have limited lifetime (Hauser, Col. 1, lines 9 – 17). Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to provide the technique of Hauser to the modified system of Ala-Laurila, Brown and Brown in order to provide a secure and compact authentication protocol between a user and the authentication server without sacrificing any of the important advantages of the known systems.

Regarding claim 10, the claim is interpreted and rejected for the same reason as set forth in claim 4.

8. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila in view of Brown and further in view of Brown (US 5,689,563) as applied to claim 13 above and further in view of Norefors et al. (US 6,370,380) and further in view of Jetzek (US 6,539,227 B1).

Regarding claim 14, Ala-Laurila in view of Brown and further in view of Brown (US 5,689,563) as applied to claim 13 above does not specifically disclose the authentication protocol engine to apply the second ticket and a group identity shared by the first and the second access points to establish a second secured session with the second access point. In an analogous art, Norefors discloses that the mobile terminal re-encrypts the security token using an encryption key that it shares with the second access point then applying in the message a hash code, which is a key that is shared only by the two access points to establish a secure handover between the mobile terminal and the second access point (AP<sub>NEW</sub>) (Norefors, Col. 2, lines 17 – 34 and Col. 4, lines 13 – 38). Therefore it would have been obvious to one of ordinary skill in the art at the time the

invention was made to provide the technique of Norefors to the modified system of Ala-Laurila, Brown and Brown in order to protect communications associated with a mobile terminal against unauthorized intrusion when the mobile terminal undergoes a handover from one access point to another.

However, Ala-Laurila in view of Brown and further in view of Brown and further in view of Norefors as applied above does not specifically disclose that the group identity identifying the first and second access points belong to the same group, and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket. In an analogous art, Jetzek discloses that the group identity identifying the first and second access points belong to the same group (groups of cells, base stations or other transmission sources having softzone identification number, softzone ID, Jetzek, Col. 6, line 66 through Col. 7, line 3), and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket (soft handoffs are permitted only between members within the group having the same softzone ID, Jetzek, Col. 7, lines 4 – 44). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the technique of Jetzek to the modified system of Ala-Laurila, Brown, Brown and Norefors in order to provide methods and system to determine which handoff type is preferred at a specific location under current radio conditions and to

control hard and soft handoff while at the same time minimizing the overhead signaling between the network and the mobile station.

9. Claims 15, 17, 18, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over the admitted prior art in view of Brown et al. (US 5,455,863), in view of Ala-Laurila et al. (US 6,587,680 B1) and in view of Brown et al. (US 6,678,733 B1).

Regarding claim 15, the admitted prior art discloses a secured wireless roaming system comprising a wired medium (Fig. 1, 112); a wireless medium (Fig. 1, 106); an authentication server (Fig. 1, 114) coupled to the wired medium; a wireless station (Fig. 1, 108) coupled to the wireless medium and an access point (Fig. 1, 100) coupled to the wireless medium and the wired medium (the admitted prior art, Page 2, line 16 through Page 3, line 6).

However, the admitted prior art does not specifically disclose wherein the access point comprises a first control unit, comprising a first authentication protocol engine to request a first ticket from the authentication server and use the first ticket to establish a first secured session with the wireless station and in response to a second ticket request from the wireless station through the first secured session, to forward the second ticket request to the authentication server and relays a resulting second ticket from the authentication server to the wireless station, wherein the second ticket is different than the first ticket and the second is used by the wireless station to establish a second secured session with another access point coupled to the wired and wireless mediums. In an

analogous art, Brown discloses wherein the access point (fixed network communication unit, Brown (US 5,455,863), Fig. 1, 130) comprises: a first control unit (a switching center, Brown (US 5,455,863), Fig. 1, 128), comprising a first authentication protocol engine (switch center comprises a database, Brown (US 5,455,863), Fig. 1, 136, Brown (US 5,455,863), Col. 5, lines 54 – 66) to request a first ticket from the authentication server and use the first ticket to establish a first secured session with the wireless station (subscriber unit and fixed network communication unit performs authentication to establish a secured session, Brown (US 5,455,863), Col. 6, lines 14 – 67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the technique of Brown to the system of the admitted prior art in order to create an encryption technique to alleviate problems associated with packetized data to be more efficient and secure.

However, the admitted prior art in view of Browns as applied above does not specifically disclose that in response to a second ticket request from the wireless station through the first secured session, to forward the second ticket request to the authentication server and relays a resulting second ticket from the authentication server to the wireless station, wherein the second ticket is different than the first ticket and the second ticket is used by the wireless station to establish a second secured session with another access point coupled to the wired and wireless mediums. In an analogous art, Ala-Laurila in view of Brown discloses that in response to a second ticket request from the wireless station

through the first secured session, to forward the second ticket request to the authentication server and relays a resulting second ticket from the authentication server to the wireless station (mobile terminal indicating to the current or old-AP that handover is required and when the message is received by the old-AP it retrieves security association parameters, SA, from its security association database and relaying a response message to the mobile terminal, Ala-Laurila, Col. 10, lines 39 – 57), wherein the second ticket is different than the first ticket and the second ticket is used by the wireless station to establish a second secured session with another access point coupled to the wired and wireless mediums (request access, first ticket, is just a request to gain access to a network but since there is no authentication the network denies access to the user, when the user request access with ticket, second ticket, the network grants access because it is already authenticated by the network, Brown (US 6,678,733 B1), Col. 11, line 22 through Col. 13, line 25). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the technique of Ala-Laurila and Brown to the modified system of the admitted prior art and Brown in order to provide service provisioning by activating an authentication code in the cellular handset authenticate the handset to a wireless network when the subscriber attempts to access the wireless network to enhance security.

Regarding claim 17, the admitted prior art in view of Brown (US 5,455,863) in view of Ala-Laurila and in view of Brown (US 6,678,733 B1) as

applied to claim 15 above discloses an encryption/decryption engine to decrypt the second ticket request (a switch center, Brown (US 5,455,863), Fig. 1, 128, comprising an encryptor/decryptor to decrypt the second ticket request, Brown, Col. 8, lines 16 – 24) before the authentication protocol engine forwards the second ticket request (after the first secured session is established old-AP forwards the request to the new-AP, Ala-Laurila, Col. 8, lines 1 – 6 and Col. 10, lines 39 – 57).

Regarding claim 18, the admitted prior art in view of Brown (US 5,455,863), in view of Ala-Laurila and in view of Brown (US 6,678,733 B1) as applied to claim 15 above discloses that the authenticating unit generating a first and a second session keys to include in the first and the second tickets and the authenticating unit encrypting the first and the second tickets with a first and a second encryption keys (Brown (US 5,455,863), Col. 3, line 63 through Col. 4, line 8).

Regarding claim 20, the admitted prior art in view of Brown (US 5,455,863), in view of Ala-Laurila and in view of Brown (US 6,678,733 B1) as applied to claim 17 above discloses the first fixed network communication unit 130 appending application specific information to the second ticket to formulate a combined message and the first fixed network communication unit encrypting the combined message with the first session key (Brown (US 5,455,863), Col. 6, lines 35 – 54).

Regarding claim 21, the admitted prior art in view of Brown (US 5,455,863), in view of Ala-Laurila and in view of Brown (US 6,678,733 B1) as applied to claim 20 above discloses that the application specific information further comprises the first fixed network communication unit 130 selected instant specific information and random challenge (RAND) (Brown (US 5,455,863), Col. 6, lines 14 – 21 and Col. 7, lines 39 – 48).

10. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over the admitted prior art in view of Brown (US 5,455,863), in view of Ala-Laurila and in view of Brown (US 6,678,733 B1) as applied to claim 15 above, and further in view of Jetzek.

Regarding claim 16, the admitted prior art in view of Brown (US 5,455,863), in view of Ala-Laurila and in view of Brown (US 6,678,733 B1) as applied to claim 15 above does not specifically disclose wherein the wireless station further comprises a second authentication protocol engine to apply the second ticket and a group identity shared by the first and a second access points to establish a second secured session with the second access point, the group identity identifying that the first and second access points belong to the same group, and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket. In an analogous art, Jetzek discloses applying the second ticket (mobile station roaming from one base station to another performing handoff) and a group identity shared by the first and the second access points to establish a second

secured session between the wireless station and the second access point, the group identity identifying that the first and second access points belong to the same group (groups of cells, base stations or other transmission sources having softzone identification number, softzone ID, Jetzek, Col. 6, line 66 through Col. 7, line 3), and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket (soft handoffs are permitted only between members within the group having the same softzone ID, Jetzek, Col. 7, lines 4 – 44). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the technique of Jetzek to the modified system of the admitted prior art, Brown, Ala-Laurila and Brown in order to provide methods and system to determine which handoff type is preferred at a specific location under current radio conditions and to control hard and soft handoff while at the same time minimizing the overhead signaling between the network and the mobile station.

11. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over the admitted prior art in view of Brown (US 5,455,863), in view of Ala-Laurila and in view of Brown (US 6,678,733 B1) as applied to claim 17 above, and further in view of Hauser.

Regarding claim 19, the admitted prior art in view of Brown (US 5,455,863), in view of Ala-Laurila and in view of Brown (US 6,678,733 B1) as applied to claim 17 above does not specifically disclose that the first and second session keys have limited lifetime. In an analogous art, Hauser teaches that

session keys have limited lifetime (Hauser, Col. 1, lines 9 – 17). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the technique of Hauser to the modified system of the admitted prior art, Brown, Ala-Laurila and Brown in order to provide a secure and compact authentication protocol between a user and the authentication server without sacrificing any of the important advantages of the known systems.

### ***Response to Arguments***

12. Applicant's arguments with respect to claims 1 – 27 have been considered but are moot in view of the new ground(s) of rejection.

### ***Conclusion***

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2687

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Un C Cho whose telephone number is (571) 272-7919. The examiner can normally be reached on M ~ F 8:00AM to 4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester Kincaid can be reached on (571) 272-7922. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
**SONNY TRINH**  
**PRIMARY EXAMINER**

Un C Cho  
Examiner  
Art Unit 2687

4/8/05 uc